REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed August 12, 2004. In the Office Action, claims 1-29 were rejected under 35 U.S.C. §103(a). Applicant respectfully traverses these rejections and requests reconsideration of the allowability of claims 1-29.

Objection of Disclosure

The specification was objected to on the grounds that an article was missing on page 5, line 9 of the specification. More specifically, the phrase "Figure 30 is first embodiment..." should read "Figure 30 is a first embodiment..." Based on the following revisions, Applicant respectfully requests the Examiner to withdraw the outstanding objection.

Double Patenting Rejection

Claims 1-8, 15-20, 22 and 25 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting based on the outstanding claims set forth in a co-pending Continuation-In-Part (CIP) application (Application No. 09/904,962). In the event that the Examiner agrees that the claims as amended are in condition for allowance, at that time, Applicant respectfully offers to submit an executed terminal disclaimer to overcome the obviousness-type double patenting rejection.

Rejection Under 35 U.S.C. § 103

A. §103 REJECTION OF CLAIMS 15-17, 20-22 AND 24

Claims 15-17, 20-22 and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Coppersmith (U.S. Patent No. 6,243,470) in view of Ritter (U.S. Patent No. 5,727,062). Applicant respectfully traverses the rejection.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of

success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143, p.2100, 124(8th Ed., rev.1,Feb 2003); see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988).* Herein, the combined teachings of the cited references fail to describe or suggest all the claim limitations.

With respect to independent claim 15, the Office Action states that Coppersmith "does not expressly disclose the input data as being segmented into random sized blocks." *See Page 4 of the Office Action.* Applicant agrees that Coppersmith offers no such disclosure. However, Applicant disagrees with the Office Action that Ritter provides disclosure of the input data as being segmented into random sized blocks using an encryption key for such segmentation as claimed.

First, based on the teachings of Coppersmith and Ritter, a *prima facie* case of obviousness has not been established because the combined teachings of Coppersmith and Ritter fail to describe or suggest all the claim limitations. The lack of suggestion of all of the claim limitations is due, in part, to the fact that both Coppersmith and Ritter teach away from the claimed limitation of segmenting the input data into *random sized blocks using an encryption key.* It is expressly noted in Coppersmith that "the process of FIG. 3 does not show the user entering particular values to be used for the variables (block size, key size, and the number of rounds) defined for the cipher of the present invention, nor the value to be used for the key. The *user will have been prompted to enter these values...." See Col. 7, lines 33-43; Emphasis added.* In summary, Coppersmith teaches a cipher processing data blocks of a constant, pre-defined size, and thus, teaches away from segmented into random sized blocks through use of an encryption key.

Ritter teaches blocks of a pre-defined size except for the last block, which may be partially filed. More specifically, column 11, lines 64-67 of Ritter states that "Fig. 1 is an example of an 80-bit block cipher built solely from variable size layers. This makes the cipher easily extendible (in byte-by-byte steps) to arbitrary size, either at design-time or dynamically during operation." This statement, however, indicates that Ritter creates a block cipher to fit the size of an existing length of input data or available data to be encrypted. A block of a variable

size comes into effect *only if* the length of the input data is different from some pre-defined block size, and thus, Ritter teaches segmentation where *only the last block is partially filled.* Emphasis added.

As a result, neither Coppersmith nor Ritter, alone or in combination, teaches or suggests performance of a stream cipher operation *on input data segmented into random sized blocks using an encryption key. Emphasis added.* As noted above, Coppersmith teaches blocks having a pre-defined length while Ritter teaches blocks of a pre-defined size except for the last block, which may or may not be partially filed. In effect, Ritter does not teach or even suggest random sized blocks as claimed, but instead teaches pre-defined blocks.

As an example, in the case of Ritter, if N is the number of input data elements to be encrypted, and if C is the block size, then in the case of Ritter, the sequence of block sizes processes are C, C, C, ..., C, x, where $x < C$ if N is not an integral multiple of C. In the case of Coppersmith, the block size is first defined before the encryption begins. For the claimed invention, however, the block sizes used are n_1, n_2, n_3, n_4, ... , which are all different and form a pseudo-random sequence. This sequence is not a static sequence and varies based at least in part on the encryption key to form a different pseudo-random sequence.

Secondly, to provide clarity as to the differences between the claimed invention and the combined teachings of Coppersmith and Ritter, claims 21-22 have been amended to include the limitation that segmentation of the input data is such that some or all of the blocks may vary in length from a proceeding block. Consideration of these amended claims is respectfully requested.

Therefore, Applicant respectfully submits that neither Coppersmith nor Ritter, alone or in combination, disclose or suggest each and every limitation set forth in independent claims 15 as well as those limitations set forth in dependent claims 16-17, 20-22 and 24. Withdrawal of the outstanding §103(a) rejection is respectfully requested.

B. §103 REJECTION OF CLAIMS 1-4, 14, 18 AND 19

Claims 1-4, 18 and 19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Coppersmith in view of Ritter and Reardon (U.S. Patent No. 6,212,635). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established.

As the Examiner is aware, to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. *See MPEP §2143; see also In Re Fine, 873 F. 2d 1071, 5 U.S.P.Q.2D 1596 (Fed. Cir. 1988).* Herein, at a minimum, the combined teachings of the cited references do not describe or suggest all the claim limitations.

With respect to independent claim 1, the Office Action states that Coppersmith and Ritter collectively disclose "a first software routine to divide incoming plain text into variable-sized blocks." *See Page 6 of the Office Action.* Applicant respectfully disagrees with the contention as noted above because neither Coppersmith nor Ritter describes or suggest pre-defined block sizes as noted above. However, none of these references, including Reardon (USP 6,212,635), suggest variable-sized blocks of which at least three blocks are divided with three different sizes as claimed. Hence, withdrawal of the §103(a) rejection as applied to claim 1 is respectfully requested.

Moreover, as set forth in dependent claims 2 and 18, Applicant respectfully agrees that Coppersmith also does not teach altering the block size based on an encryption key and an internal identifier. *See Page 7 of the Office Action.* However, Applicant disagrees with the Office Action that Ritter provides any disclosure of forming random-sized blocks of the input data b*ased on an encryption key. Emphasis added.*

Rather, Applicant respectfully submits that neither Coppersmith nor Ritter, alone or in combination, disclose or suggest: (1) the first software routine *produces the variable-sized*

blocks based on the encryption key, and (2) a stream cipher operation processed by the logic to produce random-sized blocks of the input data b*ased on an encryption key, the unique internal identifier and an output of a first non-linear function. Emphasis added.* Rather, both Coppersmith and Ritter involve pre-defined block sizes, and for Ritter, the block size of the last block is the only block size that changes. These sizes are not based at all on either the encryption key or the unique internal identifier as claimed. The same analysis applied to Reardon as well.

Therefore, Applicant respectfully submits that neither Coppersmith, Ritter nor Reardon, alone or in combination, disclose or suggest each of the limitations set forth in independent claim1 as well as dependent claim 2 and 18. Moreover, Applicant respectfully traverses the rejection of dependent claims 3-4 and 19, but believes that the grounds for traverse need not be enumerated based on the allowability of pending claims 1, 2 and 18. Withdrawal of the outstanding §103(a) rejection is respectfully requested and allowance of claims.

C. §103 REJECTION OF CLAIMS 5-13, 23 AND 25-26

Claims 5-13, 23, 25 and 26 were rejected under 35 U.S.C. §103(a). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established for these claims. However, based on the dependency of claims 5-13 and 23 as well as the allowability of independent claims 1 and 15, Applicant believes that no further discussion as to the grounds for traverse is warranted. Applicant reserves the right to present such arguments in an Appeal is warranted. Withdrawal of the §103(a) rejection as applied to claims 5-13, and 23 is respectfully requested.

With respect to claims 25-26, Applicant respectfully traverses the rejection because neither Coppersmith, Ritter, Reardon nor Moskowitz (U.S. Patent No. 5,822,432), alone or in combination, suggest decrypting blocks of the cipher text using *the decryption key, the percentage of random data and the unique internal identifier* in order to recover corresponding blocks of plain text. Emphasis added.

D. §103 REJECTION OF CLAIMS 27-29

Claims 27-29 were rejected under 35 U.S.C. §103(a). Applicant respectfully traverses the rejection because a *prima facie* case of obviousness has not been established for these claims. However, claims 27-29 have been cancelled without prejudice and claims 30-32 have been added. Claims 30-32 are substantially similar to claims 1, 2 and 4, but include the limitation that the first software routine divides incoming plain text into variable-sized blocks *with each block varying in size. Emphasis added.* Consideration of the newly added claims is respectfully requested.

Conclusion

In view of the remarks made above, it is respectfully submitted that pending claims 1-29 define the subject invention over the prior art of record. Thus, Applicant respectfully submits that all the pending claims are in condition for allowance, and such action is earnestly solicited at the earliest possible date. *The Examiner is respectfully requested to contact the undersigned attorney by telephone at the telephone number listed below if it is believed that, after review, such claims are still not in condition for allowance. This telephone conference would greatly facilitate the examination of the present application.*

To the extent necessary, a petition for an extension of time under 37 C.F.R. §1.17 is hereby made. Please charge any shortage in fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 01/10/2005

By _____
William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: 01/10/2005

FACSIMILE

☒ *transmitted by facsimile to the Patent and Trademark Office.*

Susan McFarlane 01/10/2005
Susan McFarlane *Date*